AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-48. (Cancelled)

49. (Currently amended) A method for managing a database system, wherein the database system includes sensitive users, normal database administrators, and security officers, comprising:

receiving a command to perform an administrative function involving a user within the database system;

determining if the user is a sensitive user who is empowered to access sensitive data in the database system;

if the user is not a sensitive user, and if the command is received from a normal database administrator for the database system, allowing the administrative function to proceed;

if the user is a sensitive user, and if the command is received from a normal database administrator, preventing the normal database administrator from performing the administrative function involving the sensitive user; and

if the user is a sensitive user, and if the command is received from a security officer who is the only database administrator empowered to perform administrative functions involving sensitive users, performing the administrative function.

50. (Original) The method of claim 49, further comprising:

receiving a request to perform an operation on a data item in the database system;

if the data item is a sensitive data item containing sensitive information and if the request is received from a sensitive user who is empowered to access sensitive data, allowing the operation to proceed if the sensitive user has access rights to the sensitive data item; and

if the data item is a sensitive data item and the request is received from a user who is not a sensitive user, disallowing the operation.

51. (Original) The method of claim 50, wherein if the data item is a sensitive data item, if the operation is allowed to proceed, and if the operation involves retrieval of the data item, the method further comprises decrypting the data item using an encryption key after the data item is retrieved.

52. (Original) The method of claim 51, wherein the encryption key is stored along with a table containing the data item.

53. (Original) The method of claim 52, wherein the encryption key is stored in encrypted form.

54. (Original) The method of claim 49, wherein if the user is not a sensitive user, and if the command to perform the administrative function is received from a security officer, the method further comprises allowing the security officer to perform the administrative function on the user.

55. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for managing a database system, wherein the database system includes

sensitive users, normal database administrators, and security officers, the method comprising:

receiving a command to perform an administrative function involving a user within the database system;

determining if the user is a sensitive user who is empowered to access sensitive data in the database system;

if the user is not a sensitive user, and if the command is received from a normal database administrator for the database system, allowing the administrative function to proceed;

if the user is a sensitive user, and if the command is received from a normal database administrator, preventing the normal database administrator from performing the administrative function involving the sensitive user; and

if the user is a sensitive user, and if the command is received from a security officer who is the only database administrator empowered to perform administrative functions involving sensitive users, perfoming the administrative function.

56. (Original) The computer-readable storage medium of claim 55, wherein the method further comprises:

receiving a request to perform an operation on a data item in the database system;

if the data item is a sensitive data item containing sensitive information and if the request is received from a sensitive user who is empowered to access sensitive data, allowing the operation to proceed if the sensitive user has access rights to the sensitive data item; and

if the data item is a sensitive data item and the request is received from a user who is not a sensitive user, disallowing the operation.

57. (Original) The computer-readable storage medium of claim 56, wherein if the data item is a sensitive data item, if the operation is allowed to proceed, and if the operation involves retrieval of the data item, the method further comprises decrypting the data item using an encryption key after the data item is retrieved.

58. (Original) The computer-readable storage medium of claim 57, wherein the encryption key is stored along with a table containing the data item.

59. (Original) The computer-readable storage medium of claim 58, wherein the encryption key is stored in encrypted form.

60. (Original) The computer-readable storage medium of claim 55, wherein if the user is not a sensitive user, and if the command to perform the administrative function is received from a security officer, the method further comprises allowing the security officer to perform the administrative function on the user.

61. (Currently amended) An apparatus that manages a database system, wherein the database system includes sensitive users, normal database administrators, and security officers, comprising:

a command-receiving mechanism configured to receive a command to perform an administrative function involving a user within the database system;

an execution mechanism configured to,

determine if the user is a sensitive user who is empowered to access sensitive data in the database system;

allow the administrative function to proceed, if the user is not a sensitive user, and if the command is received from a normal database administrator for the database system;

prevent a normal database administrator from performing the administrative function involving the sensitive user, if the user is a sensitive user, and if the command is received from the normal database administrator; and to

allow the administrative function to proceed, if the user is a sensitive user, and if the command is received from a security officer who is the only database administrator empowered to perform administrative functions involving sensitive users.

62. (Currently amended) The apparatus of claim 61,

wherein the command-receiving mechanism is configured to receive a request to perform an operation on a data item in the database system;

wherein the execution mechanism is configured to,

allow the operation to proceed, if the data item is a sensitive data item containing sensitive information and if the request is received from a sensitive user who is empowered to access sensitive data, and if the sensitive user has access rights to the sensitive data item; and to

disallowing the operation, if the data item is a sensitive data item, and the request is received from a user who is not a sensitive user.

63. (Currently amended) The apparatus of claim 62, further comprising a decryption mechanism, wherein if the data item is a sensitive data

item, if the operation is allowed to proceed, and if the operation involves retrieval of the data item, the decryption mechanism is configured to decrypt the data item using an encryption key after the data item is retrieved

64. (Currently amended) The apparatus of claim 63, wherein the encryption key is stored along with a table containing the data item.

65. (Currently amended) The apparatus of claim 64, wherein the encryption key is stored in encrypted form.

66. (Currently amended) The apparatus of claim 61, wherein if the user is not a sensitive user, and if the command to perform the administrative function is received from a security officer, the execution mechanism is configured to allow the security officer to perform the administrative function on the user.